XEDAPEN OROKORRAK

EUSKAL HERRIKO UNIBERTSITATEA

2239

ERABAKIA, 2013ko apirilaren 25ekoa, UPV/EHUko Gobernu Kontseiluarena, Universidad del País Vasco / Euskal Herriko Unibertsitatearen (UPV/EHU) Informazioaren Segurtasun Politika dokumentua onartzea.

AURREKARIAK

UPV/EHUk informazio eta komunikazio teknologiak (IKT) erabiltzen ditu bere helburuak betetzeko aurrera eramaten dituen jardueren laguntza tresna gisa. Beraz, IKT sistemak eta baliabideak arduraz kudeatu behar dira eta, orobat, informazioa eta horren euskarri diren sistema eta zerbitzu elektronikoak babesteko neurriak hartu, beren eskuragarritasunean, konfidentzialtasunean, osotasunean edo kontserbazioan eragina izan dezaketen ustekabeko kalteei zein nahita egindako kalteei aurre egin ahal izateko.

Esandakoari erantzuten dio 11/2007 Legeak, ekainaren 22koak, herritarrek zerbitzu publikoak baliabide elektronikoez erabiltzeari buruzkoak, 42.2 artikuluan; eta horretarako arautu zen Segurtasun Eskema Nazionala (ENS), helburu duena baliabide elektronikoak segurtasunez erabiltzeko politikarako printzipioak eta baldintzak ezartzea, horien bidez informazioa behar bezala babesteko.

Zehatzago esanda, ENSk, 11. artikuluan, dio administrazio publikoetako organo goren guztiek informazioaren segurtasun politika xedatu behar dutela, kasuan kasuko organoko titularrak onartu beharrekoa.

UPV/EHUren Informazioaren Segurtasun Politikaren helburua da, azken finean, informazioaren kalitatea bermatzea eta zerbitzuak modu jarraituan ematea, betiere prebentzio neurriak hartuz, eguneroko jarduna ikuskatuz eta gerta daitezkeen gorabeherei azkar erantzunez.

Administrazio Elektronikoko Batzordea, martxoaren 6ko bileran, UPV/EHUren Informazioaren Segurtasun Politikari buruzko zirriborroaren alde agertu zen. Zirriborro hori Gobernu Kontseiluari aurkeztu zitzaion ondoren, 2013ko martxoaren 21eko ohiko bileran, eta zuzenketak aurkezteko epea ireki zen, apirilaren 12ra arte.

2013ko martxoaren 21eko testuari zuzenketak egiteko epea amaitu da eta ez da bat ere aurkeztu.

Horrela, bada, idazkari nagusiaren proposamenari jarraituz, Gobernu Kontseiluak honakoa

ERABAKI DU

Lehenengoa.– UPV/EHUren Informazioaren Segurtasun Politika onartzea, eranskinean adierazitako moduan.

Bigarrena.– Euskal Herriko Agintaritzaren Aldizkarian argitaratzeko agindua ematea. UPV/EHUren Informazioaren Segurtasun Politika EHAAn argitaratu eta biharamunean jarriko da indarrean.

Leioa, 2013ko apirilaren 25a

Errektorea,
IÑAKI GOIRIZELAIA ORDORIKA.

Idazkari nagusia,
JOSE LUIS MARTÍN GONZÁLEZ.

INFORMAZIOAREN SEGURTASUN POLITIKA UPV/EHUN

Aurrekariak

Informazioa ezinbesteko aktiboa da UPV/EHUko jarduera eta zerbitzu gehienak bete eta gestionatzeko, eta, beraz, arduraz babestu eta administratu behar da eta bermatu informazio sistema ez dela etengo. Informazioaren babesa are garrantzitsua da egungo egoeran, informazio sistemarako arrisku eta mehatxu berriak ekarri baitituzte administrazio jardunean ohiko bihurtu diren informazio eta komunikazio teknologiek.

Informazioaren segurtasun politika honek informazioaren segurtasunaren arloan indarrean dauden legeetan du oinarri, ezinbestean bete beharrekoetan, eta, hain zuzen ere, ondokoetan: 11/2007 Legea, ekainaren 22koa, herritarrek zerbitzu publikoak baliabide elektronikoez erabiltzeari buruzkoak (aurrerantzean LAE); 3/2010 Errege Dekretua, urtarrilaren 8koa, Administrazio Elektronikoaren Esparruan Segurtasun Eskema Nazionala arautzen duena (aurrerantzean ENS), helburu duena baliabide elektronikoak segurtasunez erabiltzeko politikarako oinarrizko printzipioak eta gutxieneko baldintzak ezartzea horien bidez informazioa behar bezala babesteko eta baliabidekok konfiantzaz erabiltzeko beharrezko diren baldintzak sortzeko.

ENSk, 11. artikuluan, dio administrazio publikoetako organo goren guztiek informazioaren segurtasun politika xedatu behar dutela, kasuan kasuko organoko titularrak onartu beharrekoa. Beraz, agiri honek arau izaera izango du eta UPV/EHUko Gobernu Kontseiluari aurkeztu behar zaio hark onar dezan.

Bestalde, UPV/EHUk, 2012-2017 Plan Estrategikoan (IV. ardatza: Gobernantza eta kudeaketa) jasotakoari jarraituz, administrazio elektronikoa ezartzeko proiektua ari da garatzen Idazkaritza Nagusiak bultzatuta eta IKT Gerenteordetzarekin koordinatuta, eta agiri hau horren parte da. Horrela, unibertsitatearen ildo estrategikoetako bat da gestioaren kalitatea eta eraginkortasuna hobetzea, betiere, konpromiso sendoa izanik informaziorako eta zerbitzu eta sistema elektronikoetarako ondokoak bermatzea: konfidentzialtasuna, osotasuna, benetakotasuna, trazabilitatea eta kontserbazioa.

1. artikulua.– Xedea eta ezarpen eremua.

Informazioaren segurtasun politika honen xedea da UPV/EHUren informazio sistemaren maila guztiak definitzea eta maila guztietan arautzea, hain zuzen ere Estatutuetako 1. artikuluaren babesean UPV/EHUk goi mailako hezkuntza arloko zerbitzu publikoa emateko behar dituen informazio sistema guztietakoak.

Informazioaren Segurtasun Politika hau ezarriko zaie hala UPV/EHUko IKT zerbitzu, sistema eta bestelako baliabideei nola unibertsitatearen prozesuei sostengua ematen dieten eta beren baitan kokatutako informazio aktiboetan eragina duten beste guztiei.

UPV/EHUko IKT baliabideen helburua da irakaskuntzari, ikerketari eta unibertsitatearen funtzionamendurako beharrezko diren administrazio lanei laguntza ematea. Unibertsitatearen IKT baliabideak dira: bere jabetzako sistema nagusi eta sailetako guztiak, lan estazioak, lanpostuetako ordenagailuak, inprimagailuak eta periferiko eta irteera gailu guztiak, lokalizazio sistemak, barneko eta kanpoko sareak, erabiltzaile anitzeko sistemak eta komunikazio zerbitzuak (ahotsaren, irudiaren, datuen eta dokumentuen transmisio telematikoa eta biltegiratze sistemak, bai eta horietako sistema edo azpiegituretan instalatuta dauden informatikako aplikazioak (softwarea) ere.

Horri jarraituz, ez dira unibertsitatearen IKT baliabide izango, eta, beraz, ez dira informazioaren segurtasun politika honen menpe egongo, norberak erositako eta UPV/EHUren inbentarioan sar-

tuta ez dauden ordenagailuak. Hala ere, norberaren ordenagailua erabilita erakundearen sarean sartuz gero, Informazioaren Segurtasun Politika honen menpe eta hori garatzeko zehaztutako gainontzeko arau eta jarraibideen menpe egongo dira.

Informazioaren Segurtasun Politika UPV/EHUko IKT baliabideak erabiltzen dituzten pertsona guztiei ere ezarriko zaie, edozein izanda ere laneko atala, ikastegia, saila, institutua, egitura, erakundea, unitatea edo zerbitzua (barneko zein kanpokoa).

2. artikulua.– Printzipioak.

Informazioaren segurtasun politika honek babeserako ondorengo oinarrizko printzipioak ditu euskarri, eta horiexek izango dira UPV/EHUk informazioaren segurtasunerako egingo dituen jarduera guztien zutabe.

a) Segurtasuna elementu guztiei dagokie.

Informazioaren tratamenduan hainbat elementuk hartzen dute parte: pertsonek, baliabide teknikoek, baliabide materialek eta antolakuntzako baliabideek: elementu guzti-guztion menpe dagoen prozesu baten emaitza da informazioaren segurtasuna.

b) Arriskuen gestioa.

Informazioaren segurtasunaren gestioa arriskuen gestioan dago oinarrituta, eta helburu izan behar du gutxieneko maila onargarrien barruan mantentzea arrisku maila, horretarako, batetik, segurtasuneko neurri egokiak ezarrita, etengabe eguneratuak informazioaren tratamendurako erabilitako aplikazio eta zerbitzu guztien bizi zikloan, eta, bestetik, oreka eta proportzionaltasuna ezarrita datuen izaeraren, datu horien tratamenduaren, egon daitezkeen arriskuen eta ezarri beharreko segurtasun neurrian artean.

c) Prebentzioa, erantzuna eta informazioa berreskuratzea.

Sistemaren segurtasunerako ezinbestekoa da prebentzioa, arriskuak antzemateko eta beharrezko zuzenketak egiteko, hartara mehatxuak ez gauzatzea eta informazio sistemetako eta zerbitzuetako datuetan eragin larririk ez izatea lortzeko.

Segurtasuneko gorabeherei erantzuna emateko sistema izan behar da, gorabeheroi denboraz hartzeko aurre. Bestalde, beharrezkoa da informazioa berreskuratu eta zerbitzuak zuzentzeko bitartekoak izatea, segurtasuneko gorabeheraren baten eraginez ohiko baliabideak zerbitzutik kanpo geratuz gero eskura izateko konponbideak.

d) Defentsa lerroak.

Babeserako estrategia ezartzen da segurtasun maila askoz osatua. Neurriak antolaketakoak, operatiboak, fisikoak eta logikakoak dira, eta horien guztien antolaketa egokiaren bidez, lortzen da horrelako mailaren batean segurtasunak kale eginez gero, gainontzekoetan eraginik ez izatea. Era berean, informazio sistemak diseinatu eta osatzean kontuan izan behar da sistemak berak izan behar duela modurik segurtasuna bermatzeko.

e) Koordinazioa eta elkarlana.

Informazioaren segurtasun arduradunak elkarlanean aritu beharko dira informazioaren segurtasun neurriak ezarri eta kontrolatzeko zereginean. Elkarlan hori UPV/EHUko ekimen eta jarduera guztietarako izan behar da.

f) Aldain aldiko ebaluazioa eta etengabeko hobekuntza.

Informazioaren segurtasun gestioa aldian-aldian ebaluatu behar da eta etengabe eguneratu eta monitorizatu sistema eraginkorra izan dadin, arriskuak ez ezik, babes sistemak berak be etengabe ari baitira aldatzen.

g) Informazioaren sailkapena.

UPV/EHUk informazio aktibo guztiak sailkatu eta inbentariatuko ditu oinarri hartuta bakoitzaren izaera, bai eta informazioaren arduradunak ere; guztia informazioaren segurtasun politika honetan zehaztutakoaren babesean. Ezarri beharreko babes maila eta neurriak sailkapen horretako emaitzen araberakoak izango dira.

3. artikulua.– Eginkizunak eta erantzukizunak.

UPV/EHUren informazioaren segurtasun politika hau eta informazioaren segurtasunaren arloko gainontzeko arau eta jarraibideak ezartze aldera, antolaketako egitura zehaztu da horrela eginkizunak banatzeko eta horren araberako erantzukizunak zehazteko. Informazioaren segurtasunari buruzko agiri honetan eta ENSn adierazitako erantzukizunak Estatutuetan edo bestelakoen jasotakoaren arabera hala dagokion kargudunaren edo lanpostuan ari denarena izango da.

Plantillan egindako edozein aldaketaren ondorioz kendu edo aldatu egiten bada ENSren ezarpenarekin zerikusia daukan lanposturen bat, zehaztu egin beharko da, nahitaez, zein lanposturi esleitzen zaizkion eginkizun horiek.

1) Informazioaren Segurtasun Batzordea.

Informazioaren Segurtasun Batzordea kide anitzeko organoa da, informazioaren segurtasun arloko gaiak gestionatu, koordinatu, ezarri eta onartzen dituena. Batzordeko kide izango dira:

• Informazioaren arloko arduraduna edo hark eskuordetza emandako pertsona (batzordeburua izango da).

• Informazioaren segurtasuneko arduraduna (idazkaria izango da).

• Informazio Zerbitzuetako arduradunen ordezkari bat, kontuan izanda zein gai aztertuko den bileran. Gehienez ere zerbitzuetako 4 ordezkari egongo dira, arloko arduradun gorenek aukeratuak UPV/EHUko Estatutuetako 180. artikuluan jasotakoari jarraituz.

• Informazio Sistemetako arduradun bat, gerenteak edo eskuordetutako pertsonak, aukeratua.

UPV/EHUko zerbitzu eta unitate guztiek dute Informazioaren Segurtasun Batzordeari eskatutako informazioa eta laguntza emateko betebeharra. Ondokoak dira batzordearen eginkizun eta erantzukizunak:

a) Informazioaren segurtasunaren arloko estrategia eta lan lerroak osatzea eta bultzatzea.

b) Etengabeko hobekuntza bultzatzea informazioaren segurtasunaren gestio sisteman.

c) Gobernu Kontseiluari ENSarekin lotura duten arautegi eta arau orokorrak eta, egoki izanez gero, UPV/EHUko informazioaren segurtasunerako teknikak aurkeztea kontseiluak onar ditzan.

d) Informazioaren segurtasun tekniketarako irizpideak osatzea eta jarraipena egitea, Gobernu Kontseiluak onartutako arau orokorrak garatze aldera.

e) Informazioaren Segurtasun Politika eta gainontzeko arau orokorrak osatzea, gainbegiratzea eta jarraipena egitea, eta Gobernu Kontseiluari beharrezko diren aldaketak proposatzea.

f) Informazioaren Segurtasun Politika eta UPV/EHUk informazioaren segurtasunerako onartutako arau eta irizpideak zabaltzea.

f) Informazioaren Segurtasun Politika eta UPV/EHUk informazioaren segurtasunerako onartutako arau eta irizpideak ezartzean sor daitezkeen arazoak aztertu eta ebaztea.

h) Informazioaren Segurtasun Politika eta arlo horretako arau eta irizpideak betetzen ez direnean, horren berri ematea organo eskudunari eta, behar izanez gero, diziplina neurriak ezartzea eskatzea.

i) INSaren jarraipenerako lanak gainbegiratzea eta onartzea.

j) Informazio sistemetan izandako gorabeherak ikertzea eta aztertzea, bai eta ezarri diren neurriak ere.

k) Gobernu Kontseiluari urtero txostena aurkeztea, Informazioaren Segurtasun Politikaren gestioari buruzkoa; txostenean jaso ahalko dira informazioaren segurtasun arloan izandako gorabeherak.

2) Informazioaren arduraduna.

Informazioaren arduraduna UPV/EHUko idazkari nagusia izango da. Ondokoak dira bere eginkizun eta erantzukizunak:

a) Informazioaren segurtasunak bete beharreko baldintzak zehaztea.

b) Arriskuen analisian jasotako informazio aktibo bakoitzerako behar den segurtasunaren dimentsioa definitzea (eskuragarritasuna, konfidentzialtasuna, osotasuna, benetakotasuna eta trazabilitatea) eta horietako bakoitzari dagokion maila.

c) Hirugarrenekin egiten diren kontratuetan segurtasun klausulak sartzen direla eta bete egiten dituztela zaintzea.

d) Organo eskudunek emandako gainontzeko eginkizunak.

3) Informazio zerbitzuetako arduradunak.

Informazio zerbitzuetako arduradunak UPV/EHUko zerbitzuetako buruak izango dira.

Ondokoak izango dira zerbitzuko arduradunaren eginkizunak:

a) Zehaztea informazioaren tratamenduaren arloan zerbitzuan bermatu beharreko segurtasun baldintzak.

b) Definitzea arriskuen analisian jasotako zerbitzuek dituzten segurtasun premiak, segurtasunaren dimentsioak (eskuragarritasuna, konfidentzialtasuna, osotasuna, benetakotasuna eta trazabilitatea) eta horietako bakoitzari dagokion maila.

c) Egon daitezkeen gorabeherek izan dezaketen eragina aztertzeko lanean laguntza ematea, eta gorabehera horietarako estrategiak eta babes neurriak proposatzea.

4) Informazio sistemen arduradunak.

Informazio sistemetako arduradunak IKT zerbitzuetako buruak izango dira. Ondokoak dira eginkizunak eta erantzukizunak:

a) Bere erantzukizunpeko baliabideak kontrolpean daudela bermatzea.

b) Bere erantzukizunpeko sistemetan segurtasun baldintzak ezartzea.

c) Segurtasun prozesuak betetzea bere eraginpeko arloan.

d) Segurtasun fisikoa eta logikoa ezartzea bere arloan.

e) Segurtasuneko, DPBLko eta arriskuen gestioko auditorietan laguntzako ematea.

5) Informazioaren segurtasuneko arduraduna.

Informazioaren segurtasuneko arduraduna gerentea izango da edo hark eskuordetutako pertsona. Ondokoak dira bere eginkizunak eta erantzukizunak:

a) Zehaztea informazioaren eta zerbitzuen segurtasunak bete behar dituen baldintzak betetzeko beharrezko diren neurriak, eta egiaztatzea ezarrita daudenak egokiak direla une oro informazioa eta zerbitzuak babesteko.

b) Zehaztea sistemaren kategoria kontuan hartuta ENSaren I. eranskinean jasotako prozedura eta ezarri beharreko segurtasun neurriak.

c) Informazio aktiboen bizi zikloan egiten diren prozedura eta eragiketa guztiak gainbegiratzea.

d) Adostea, zerbitzuetako eta sistemetako arduradunekin batera, informazio jakin baten edo zerbitzu jakin baten erabilera etetea, segurtasunean arazo larririk antzemanez gero.

e) Informazio arduradunei eta zerbitzuetako arduradunei gorabehera funtzional arinen berri ematea.

f) Gorabehera larriei buruzko txostenak egitea Informazioaren Segurtasun Batzordean aurkezteko.

g) Aldian-aldian auditoriarako eskaria egitea eta ekimen hori sustatzea, egiaztatzeko UPV/EHUk bete egiten dituela informazioaren segurtasunaren arloan dituen betebeharrak.

h) Informazioaren Segurtasun Politikaren jarraipena egitea, bai eta IKT baliabideen segurtasun fisiko eta logikoarena ere.

i) Informazioaren Segurtasun Batzordeari proposatzea segurtasunaren arloan beharrezko diren arauak eta jarraibide eta irizpide teknikoak, bai eta horietan egin beharreko aldaketak ere.

4. artikulua.– Informazioaren segurtasunaren arloko araudia.

UPV/EHUk informazioaren segurtasunerako araudi esparru bat ezarri du, mailakatua, eta hartara, agiri honetan jasotako helburuak banan-banan garatuko dira:

1) Lehenengo maila: informazioaren Segurtasun Politika eta arau orokorrak.

2) Bigarren maila: informazioaren segurtasunerako jarraibideak eta gidalerroak. Agiri bilduma, prozedura jakin batean jasota ez dagoen gorabeheraren bat gertatzen denean nola jokatu azaltzen duena.

3) Hirugarren maila: informazioaren segurtasun prozedurak. Agiri bilduma, jarduera jakin bat nola bete azaltzen duena, zehatz-mehatz eta pausuz pausu azaldu ere.

4) Laugarren maila: praktika onak, aholkuak, gidak, prestakuntza ikastaroak, aurkezpenak... biltzen dituzten dokumentuak.

Informazioaren Segurtasun Politika eta arau orokorrak UPV/EHUko Gobernu Kontseiluak onartuko ditu idazkari nagusiaren eta Informazioaren Segurtasun Batzordearen proposamenari jarraituz, hurrenez hurren. Informazioaren segurtasunerako jarraibide eta gidalerro teknikoak, bigarren, hirugarren eta laugarren mailakoak, Informazioaren Segurtasun Batzordeak onartuko ditu informazioaren segurtasuneko arduradunek zerbitzuetako eta sistemetako arduradunekin lankidetzan egindako proposamenei jarraituz.

Informazioaren Segurtasun Batzordeak informazioaren segurtasunerako adostutako jarraibideak errektorearen erabaki bidez onartuko dira eta jarraibideak ez betetzeak diziplina arloko erantzukizuna izango du.

5. artikulua.– Informazio sisteman sartzea.

UPV/EHUk jendaurrean ez daukan informazioa erabiltzen duen erabiltzaile oro behar bezala identifikatuta egon behar da eta informazio horretara sartzeko beharrezko diren pribilegioak izan beharko ditu. Beraz, informazio sistemetarako sarrera kontrolatuta egon behar da eta behar bezala baimendutako erabiltzaile, prozesu, gailu eta informazio sistemak baino ezin izango dira sartu informazio sistemetan, eta kasuan-kasuan baimendutako funtzioetarako baino ez dute izango sarbiderik.

6. artikulua.– Gorabeherei erantzuna ematea eta gorabeherak erregistratzea.

Informazioaren segurtasunean gorabeherarik egonez gero, erabiltzaileek Gorabeheren Protokoloari jarraitu beharko diote; agiri hori Informazioaren Segurtasun Batzordeak onartuko du Informazioaren Segurtasun Politikan zehaztutakoari jarraituz. Mota horretako gorabeheretarako osatuko den erregistroan jaso beharko dira informazioaren segurtasunean izandako gorabehera guztiak, bai eta horiek konpontzeko ezarri diren babes neurriak ere. Erregistro hori sistemaren segurtasuna etengabe hobetzeko erabiliko da.

7. artikulua.– Harremanak hirugarrenekin.

UPV/EHUk beste administrazio publiko batzuetan betetzen dituenean zerbitzuak edo beste administrazio publiko batzuei informazioa ematen dienean, edo beste zerbitzu publiko batzuk unibertsitateko informazioan sartzen direnean, Informazioaren Segurtasun Politikaren eta arloko arauen berri emango zaie beste erakundekoei, alde bietako informazioaren segurtasun batzordeen arteko komunikazio eta koordinazio bideak ezarriko dira eta informazioaren segurtasunaren arloan egon daitezkeen gorabeherei erantzuna emateko protokoloak zehaztuko.

Era berean, UPV/EHUk hirugarrenen zerbitzuak erabiltzen dituenean edo hirugarrenei informazioa laga edo unibertsitateen informaziora sartu, Informazioaren Segurtasun Politikaren eta arloko arauen berri emango zaie, bai eta zerbitzu eta informazio horien segurtasun irizpideak ere. Hirugarrenek araudian eta irizpideetan zehaztutako segurtasun neurriak eta betebeharrak bete beharko dituzte, eta nahi dituzten prozedurak ezarri ahal izango dituzte horiek betetze aldera. Prozedura bereziak ezarriko dira gorabeherak antzeman eta konpontzeko. Bermatuta egon beharko da beste erakunde edo entitateko langileak kontzientziatuta daudela informazioaren segurtasunaren arloan, Informazioaren Segurtasun Politika honen maila berean gutxienez.

Hain zuzen ere, hirugarrenek bermatu egin beharko dute auditorien bidez neurtu daitezkeen estandarretan oinarritutako informazioaren segurtasun politika betetzen dutela, eta hirugarrenek egindako kontrolak eta ikuskapenak izan beharko dituzte egiaztatzeko polita horiek bete egiten dituztela. Era berean, kontratua bukatzean, hirugarrenak bermatu beharko du, auditoria bidez edo suntsipen/ezabatze egiaztagiriaren bidez, baliogabetu eta ezabatu egin dituela UPV/EHUren datuak.

Hirugarrenek ezin badute bete Informazioaren Segurtasun Politikan jasotako punturen bat, Informazioaren Segurtasun arduradunak txostena egingo du zehazteko zeintzuk diren arriskuak eta zelan egingo zaien aurre. Horrelakoetan, aurrera egin aurretik, onespena eman beharko du informazioaren arduradunak eta kasuan kasuko zerbitzuek.

8. artikulua.– Langileen betebeharrak eta eginkizunak.

UPV/EHUren Informazioaren Segurtasun Politikan jasotakoa eta informazioaren segurtasunaren arloko gainontzeko arau eta irizpideetan zehaztutakoa nahitaez betebeharreko aginduak dira, eta ez betetzeak diziplinaren arloko erantzukizuna ekarriko du. Beraz, UPV/EHUk konpromisoa hartzen du unibertsitateko kide guztiei arlo horretako prestakuntza emateko eta gai horretaz sentsibilizatzeko, eta behar diren baliabide guztiak jartzeko eragindako pertsona guztiei hel dakien informazioa.

9. artikulua.– Erantzukizuna informazioren segurtasunaren arloko araudia betetzen ez denean.

Informazioaren Segurtasun Batzordeak aztertu ahal izango du ea UPV/EHUko datuetan sartzeko baimena dutenek edo beren lanean datuok erabiltzen dituztenek ez duten bete Informazioaren Segurtasun Politikan eta hori garatzeko arau eta irizpideetan zehaztutako betebeharren bat.

Bete ezean, prebentzio neurriak eta neurri zuzentzaileak zehaztu dira informazio sistemak eta sareak zaindu eta babesteko, eta diziplina erantzukizuna eskatu ahal izango da.

UPV/EHUren Informazioaren Segurtasun Politika ez dela bete egiaztatuz gero, erantzukizunak argitzeko eskaria egingo dute UPV/EHUko Estatutuetan jasotako bideei jarraituz.

Prozedurak eta zehapenak diziplina araubideari buruzko legedian jasotakoak izango da, administrazio publikoetako langileei buruzkoan edo UPV/EHUk berak onartutakoan jasotakoak.

XEDAPEN GEHIGARRIA

Nazioko Segurtasun Eskemaren menpe dagoen sistemaren batek datu pertsonalak baldin baditu, DPBLOn eta lege hori garatzeko emandako araudietan zehaztutakoa ezarriko zaio, bai eta ENSn jasotako baldintzak ere.

XEDAPEN IRAGANKORRA

Informazioaren Segurtasun Batzordeak erabakiko du zein epe ezarriko den informazioaren segurtasun politika hau garatzeko eta politika hau oinarri hartuta jarraibide teknikoak zehazteko.

XEDAPEN INDARGABETZAILEA

Indargabetuta geratzen dira informazioaren segurtasun politika honetan jasotakoaren kontra doazen xedapen guztiak, betiere, maila berekoak edo txikiagokoak badira.

AZKEN XEDAPENA

Arautegi hau EHAAn argitaratu eta biharamunean jarriko da indarrean.

I. ERANSKINA

GLOSATEGIA

ENSko IV. eranskinean bildutako terminoak gorabehera, ondoren jasota daude agiri honetan ageri diren terminorik erabilienak, informazioaren segurtasun arlokoak, eta horietako bakoitzaren esanahia.

Aktiboa: informazio sistemaren osagai bat edo funtzio bat, nahita edo nahi gabe erasoren bat izan dezakeena eta erakundean ondorioak izan. Aktiboak dira: informazioa, datuak, zerbitzuak, aplikazioak (softwarea), ekipoak (hardwarea), komunikazioak, administrazio baliabideak, baliabide fisikoak eta giza baliabideak.

Arriskua: aktiboak izan ditzakeen mehatxuen azterketa eta mehatxu horiek gertatu eta erakundeak kalteak izateko probabilitatea.

Arriskuen analisia: eskura dagoen informazioaren erabilera sistemakoa arriskuak identifikatzeko eta arriskuak balioesteko.

Arriskuen gestioa: jarduera koordinatuak, erakundea zuzendu eta kontrolatzeko arriskuei dagokienez.

Benetakotasuna: ezaugarri bat da informazioa sortu duen erabiltzailearen nortasuna bermatzen duena edo ziurtasun osoz jakiteko bidea ematen duena datuak nork bidali edo sortu dituen.

Eskuragarritasuna: ezaugarri honen bitartez, baimendutako pertsona, erakunde edo prozesuek informaziorako sarbidea dute behar dutenean.

Informazio sistema: baliabideen multzo antolatua, informazioa bildu, biltegiratu, prozesatu, mantendu, erabili, banatu, zabaldu, eskura jarri, aurkeztu eta igortzeko.

Konfidentzialtasuna: ezaugarri honen bidez bermatzen da informazioa ez dela baimenik gabeko norbanakoen, erakundeen edo prozesuen esku jartzen edo horien artean zabaltzen.

Osotasuna: ezaugarri horren bidez bermatzen da informazio aktiboa ez dela baimenik gabe aldatu.

Prozesua: produktu edo zerbitzu bat lortzeko egindako jarduera multzo antolatua, hasiera eta amaiera zehaztua daukana, zenbait baliabide behar dituena eta azkenean emaitza bat daukana.

Segurtasun neurriak: xedapen multzoa, helburu duena informazio sistema balizko arriskuetatik babestea eta hartara segurtasuna bermatzea. Neurriak izan daitezke: prebentziokoak, disuasiokoak, babesekoak, gorabehera antzeman eta erantzuna ematekoak edo informazioa berreskuratzekoak.

Segurtasun politika: Jarraibide multzoa, dokumentu idatzian jasoa, eta erakundeak informazioa eta zerbitzuak gestionatu eta babesteko zehaztutako jarraibideak biltzen dituena.

Segurtasuneko gorabehera: ezustekoan edo gogoz kontra izandako gertakaria, informazio sistemaren segurtasunaren kalteak eragin dituena.

Segurtasuneko gutxieneko baldintzak: informazioa eta zerbitzuak bermatzeko beharrezko baldintzak.

Segurtasuneko oinarrizko printzipioak: informazio eta zerbitzuak bermatzeko egiten den edozein ekintzak bete behar dituen oinarriak.

Sistemaren kategoria: oinarrizkoa-ertaina-handia eskalaren arabera sistemari dagokion maila, ezaugarri hori oinarri hartuta sistemaren segurtasun neurriak aukeratzeko. Sistemaren kategoriak aktiboen ikuspegi osoa biltzen du, zerbitzu jakin batzuk ematera bideratua.

Trazabilitatea: ezaugarri bat da eta horren bidez erakunde baten jarduerak erakunde horri bakarrik egotzi ahal izango zaizkio.